REMARKS

The Examiner has rejected Claims 12-16, and 18 under 35 U.S.C 101 as being directed towards non-statutory subject matter. Specifically, the Examiner has stated that Claims 12-16, and 18 relate to a computer product with computer code stored on a tangible medium, this code is merely descriptive material because the code does not perform any action nor cause any action to be performed. Applicant respectfully disagrees and asserts that Claim 12 discloses "computer code for identifying a set of policies…determining whether the conditions are met…and…activating the policies whose associated conditions are determined to be met…" (emphasis added), as claimed. Applicant respectfully asserts that identifying, determining, and activating are verbs that indicate action performed by the computer code. Therefore, applicant's claimed "computer code for identifying a set of policies… [etc.]" (emphasis added), in the manner as claimed by applicant, performs an action and is not merely descriptive material, as suggested by the Examiner.

The Examiner has rejected Claims 1-5, 7, 12-16, 18, 23, 29, and 33 under 35 U.S.C. 103(a) as being unpatentable over ConSeal PC FIREWALL Technical Summary (hereinafter ConSeal), in view of Hari et al. (Detecting and resolving packet filter conflicts), in view of Coss et al. (U.S. Patent No. 6,098,172), and further in view of Chan et al. (U.S. Patent No. 6,910,028). In addition, the Examiner has rejected Claim 28 under 35 U.S.C. 103(a) as being unpatentable over ConSeal, in view of Hari et al., in view of Coss et al., in view of Chan et al., and in further view of Horvitz et al. (U.S. Patent Application No. 2003/0046421). Applicant respectfully disagrees with such rejections, especially in view of the amendments made hereinabove to the independent claims. Specifically, applicant has amended the independent claims to at least substantially include the subject matter of former dependent Claim 11 et al.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the first element of the prima facie case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner has argued that "it would have been obvious… to use Hari et al's priorities… [and] conflict resolution… in the firewall system of ConSeal," and that the "[m]otivation to do so would have been to avoid matching multiple filters with confliction actions (see Hari et al page 1204 section II." To the contrary, applicant respectfully asserts that it would not have been obvious to combine the teachings of the Hari and ConSeal references, especially in view of the vast evidence to the contrary.

The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). Although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so." 916 F.2d at 682, 16 USPQ2d at 1432.).

Specifically, applicant respectfully disagrees with the Examiner's argument that "it would have been obvious…to use Hari et al's priorities…[and] conflict resolution in the firewall system of ConSeal" in order to "avoid matching multiple filters with confliction actions [as taught in Hari]." First, the possible solutions relied on by the Examiner relate to a situation where there is "a conflict since the packets of the flow match both F_1 and F_2 [where F_1 and F_2 are different filters]" (page 1204, right column). Thus, Hari teaches possible solutions once it is determined that a packet flow matches multiple filters, and does not disclose "avoid[ing] matching multiple filters with confliction actions" (emphasis added), as the Examiner notes.

In addition, applicant respectfully points out that the Hari reference relied on by the Examiner expressly discloses that the "implicit *conflict resolution schemes*, [which include the filter prioritization noted by the Examiner,] while simple to implement, [actually] suffer from some serious drawbacks," such as "arbitrariness on the conflict resolution" and "inflexibility in filter matching"(Page 1204, Section II – emphasis added). Additionally, the Hari reference states that "such implicit conflict resolution schemes do not work in the general case" (Page 1204, Section II – emphasis added). As a result, the Hari reference discloses a solution involving using "resolve filters for each pair of conflicting filters" (see page 1205, right column), and not filter prioritization, as noted by the Examiner. Thus, applicant respectfully asserts that it would not have been obvious to combine a prioritization technique that "do[es] not work in the general case," as taught in Hari, with that taught by ConSeal, and therefore no suggestion or motivation exists to combine such references.

More importantly, applicant respectfully asserts that the third element of the *prima facie* case of obviousness has also not been met by the prior art reference relied on by the Examiner. For example, with respect to the independent claims, the Examiner has relied on page 1204, section II from the Hari reference, excerpted in part below, to make a prior art showing of applicant's claimed technique "wherein a first policy with a higher priority has a first condition associated therewith that is different from a second condition associated with a second policy with a lower priority such that the first policy and second policy are activated under different priority-related conditions" and "identifying currently executed security actions, determining whether a conflict exists between the currently executed security actions, and resolving any conflicts between the currently executed security actions" (see this or similar, but not necessarily identical language in the independent claims).

> "a) The first matching filter in the filter database takes precedence. For example, if F_1 is stored before F2 in the

> database, then the flow goes through at 100 Mbps. On the other hand, if F_2 is stored before F_1, than most of the packets of the flow are dropped, since the flow is restricted to a BW of only 1 Mbps. This approach is commonly used to resolve conflicts in firewalls, where incoming packets are matched against filters specified in access control lists and the action is determined by the first matching filter.
> b) Assign priorities to difference filters, and use the matching filter with the highest priority. This scheme turns out to be identical to scheme a) if we sort the filters in the order of priority.
> c) Assign priorities to fields so that in case of multiple matches the filter with the most specific matching field with the highest priority is selected. For example, if the source address is given higher priority on matches than the destination address, then for packets going from network X to network Y the filter F_1 is a better match than F_2." (Hari, page 1204, section II – emphasis added)

Applicant respectfully asserts that the excerpt from Hari relied upon by the Examiner teaches a method conflict resolution where one filter is selected over other potential filters. Specifically, for conflict resolution, the Hari excerpt referenced above teaches three conflict resolution techniques. The first conflict resolution technique disclosed teaches that "[t]he first matching filter in the filter database takes precedence" (emphasis added). The second conflict resolution technique disclosed teaches to "[a]ssign priorities to difference filters, and use the matching filter with the highest priority" (emphasis added). The third conflict resolution technique disclosed teaches to "[a]ssign priorities to fields so that in case of multiple matches the filter with the most specific matching field with the highest priority is selected" (emphasis added).

Thus, the excerpt from Hari referenced above actually *teaches away* from applicant's claimed technique "wherein a first policy with a higher priority has a first condition associated therewith that is different from a second condition associated with a second policy with a lower priority such that the first policy and second policy are activated under different priority-related conditions" (emphasis added), since Hari teaches that a selection of the filters is based on the same priority-related condition [namely, condition a), b), or c) in the above excerpt]. Note that Hari does not teach that a first filter is selected based on technique a) while a second filter is selected based on technique b), etc.

In the Office Action mailed 10/12/2006, the Examiner has argued that "when a conflict arises the filter with the highest priority is selected and when only a single filter matches, i.e. no conflict, that filter is activated because it has the highest (an[d] only priority) which is a second priority related activation of a policy different than the first." Applicant respectfully disagrees. Specifically, applicant claims that "the first policy and second policy are activated under different priority-related conditions" (emphasis added), which is not met by a teaching that one policy is activated when there is no policy conflict and another policy is activated when there is a policy conflict, as the Examiner notes. Simply nowhere in the excerpt in Hari relied on by the Examiner is there any suggestion that "a first policy with a higher priority has a first condition associated therewith that is different from a second condition associated with a second policy with a lower priority such that the first policy and second policy are activated under different priority-related conditions" (emphasis added), as applicant specifically claims.

Also in the Office Action mailed 10/12/2006, applicant notes that the Examiner has simply reiterated the argument stated in the Office Action mailed 05/05/2006, namely that "the priority based system of Hari teaches that each filter (i.e. policy) has a different priority and when a packet matches more than one filter, which ever filter has a higher priority is used." Again, applicant respectfully asserts that Hari teaches, during conflict resolution, either selecting the first matching filter, the matching filter with the highest priority, or the filter with the most specific matching field with the highest priority. Again, applicant respectfully disagrees with the Examiner's rejection, since Hari teaches that a selection of the filters is based on the same priority-related condition [namely, condition a), b), or c) in the above excerpt]. Again, only applicant teaches and claims a technique "wherein ... the first policy and second policy are activated **under different priority-related conditions**" (emphasis added), as claimed.

With respect to independent Claim 28, the Examiner has relied on paragraph [0117] in Horvitz to make a prior art showing of applicant's claimed technique "wherein the conditions represent an urgency associated with an issue causing the policy to be activated."

Applicant respectfully asserts that the excerpt in Horvitz relied on by the Examiner merely discloses that "[c]lassification as used herein also is inclusive of statistical regression that is utilized to develop models of urgency or other measures of priority influencing an alerting and/or routing policy." Applicant respectfully points out that the alerting and/or routing policy disclosed in Horvitz only relates to "priorities for messages represented electronically" where such "priority of an electronic message can be classified" (see paragraph 0116). Thus, the urgency disclosed in Horvitz is associated with the message, and therefore does not even suggest that "the conditions represent an urgency associated with an issue causing the policy to be activated" (emphasis added), as claimed.

In addition, with respect to the independent claims, the Examiner has relied on Col. 7, line 60 – Col. 8, line 33 from Chan to make a prior art showing of applicant's claimed technique "wherein the conditions include a source of the policies" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully asserts that the excerpt relied upon by the Examiner merely teaches "[a] merge policy [which] represents priorities and/or mutual-exclusions" (Col. 7, lines 61-62). In addition, the excerpt teaches that "the merge policy may specify that the relative priority of rules is based on relative authority level of the originating source application of those rules" (Col. 8, lines 2-4 - emphasis added). However, the excerpt fails to disclose a technique "wherein the conditions include a source of the policies" (emphasis added), as claimed by applicant. Merely disclosing that the policy itself specifies a relative priority of rules, as in Chan, fails to suggest "conditions [that] include a source of the policies" (emphasis added), in the context claimed by applicant.

Applicant respectfully asserts that at least the first and third element of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the

ConSeal and Hari references, as noted above, and the prior art references, when combined, fail to teach or suggest all of the claim limitations, as also noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of former dependent Claim 11 et al. into the independent claims.

With respect to the subject matter of former Claim 11 et al. (now at least substantially incorporated into the independent claims), the Examiner has rejected the same under 35 U.S.C. 103(a) as being unpatentable over ConSeal, in view of Hari et al., Coss et al., Chan et al., and further in view of Porras et al. (U.S. Patent No. 6,704,874). Specifically, the Examiner has relied on the following excerpt from Porras to make a prior art showing of applicant's claimed technique "wherein the conditions include a severity of security actions associated with the policies" (see this or similar, but not necessarily identical language in the independent claims).

> "In a further aspect, alerts may be tagged with a priority indication flag formulated against the remote processing station's alert processing policy and tagged with a relevance flag that indicates the likely severity of the attack with respect to the known internal topology of the monitored network." (Col. 2, lines 46-51 - emphasis added)

In addition, applicant notes that the Examiner has argued that the above excerpt teaches that the "more severe of the attack requires a more severe action." Applicant respectfully disagrees that such excerpt teaches that a more severe attach requires a more severe action, as noted by the Examiner. In particular, such excerpt only discloses that "alerts may be tagged with a priority indication flag…[and] with a relevance flag that indicates the likely severity of the attack. Clearly, "a more severe action," as noted by the Examiner, is not disclosed in Porras, since Porras only discloses tagging alerts, and that such tags may indicate a likely severity of an attack.

Further, applicant respectfully asserts that the above excerpt from Porras merely teaches a technique where "alerts may be tagged with a priority indication flag…and tagged with a relevance flag that indicates the likely severity of the **attack**" (emphasis added). However, tagging alerts with a flag indicating the severity of the attack, as in Porras, in no way even suggests a technique "wherein the conditions include a severity of **security actions** associated with the policies" (emphasis added), as claimed by applicant.

In the Office Action mailed 10/12/2006, the Examiner argues that "Porras teaches tagging alerts with a flag indicating the severity of the attack" and that "[t]hese alerts are generated based on filtering conditions being met (see column 1 lines 51-62) and therefore are associated with the conditions being met and the more severe an attack the more severe the action in response to the attack will be."

> "In another aspect, the invention features a method of managing alerts including receiving alerts from a number of network sensors, filtering the alerts to produce one or more internal reports and consolidating the internal reports that are indicative of a common incident-to-incident report. Related incident reports may be correlated. The network sensors may format the received alerts. Filtering includes deleting alerts that do not match specified rules. The filtering rules may be dynamically adjusted. Filtering may also include tagging alerts with a significance score that can indicate a priority measure and relevance measure." (Porras Col. 1 lines 51-62 - emphasis added)

Applicant respectfully asserts that Porras merely discloses "receiving alerts from a number of network sensors" and that "[f]iltering may also include tagging alerts with a significance score that can indicate a priority measure and relevance measure" (emphasis added). However, merely tagging alerts to indicate a priority measure, as in Porras, fails to suggest a technique "wherein the conditions include a severity of security actions associated with the policies" (emphasis added), as claimed by applicant. Again, applicant respectfully asserts that the excerpts relied upon by the Examiner only disclose that alerts are tagged with a significance score, but that the excerpts fail to disclose that the "conditions include a severity of security actions associated with the policies" (emphasis added), as claimed by applicant.

Additionally, applicant again respectfully notes that nowhere in the above cited Porras excerpts is it mentioned that "the more severe an attack the more severe the action in response to the attack will be," as noted by the Examiner. Applicant respectfully disagrees with this assertion for the reasons argued above.

Thus, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. With respect to Claims 2 and 3 et al., the Examiner has relied on Page 2 of the ConSeal reference, as excerpted below in part, to make a prior art showing of applicant's claimed "determining whether a user confirms the activation of the policies" (Claim 2 et al.) and "activating the policies if the user confirms" (Claim 3 et al.)

> "ConSeal PC FIREWALL's learning modes allow rules and rulesets to be generated efficiently and straightforwardly. The Manual Learning Mode allows users to add, edit and delete their rules and tweak them according to address, service type and so on. The Checked Learning Mode prompts the user for rule generation when it encounters a packet for which it has no rule. The Unchecked Learning Mode allows users to generate rules in the background by performing their normal networking activities over a trial period." (ConSeal, Page 2 - emphasis added)

Applicant respectfully asserts that the excerpt from ConSeal relied upon by the Examiner merely teaches a technique where the "Checked Learning Mode prompts the user for rule generation when it encounters a packet for which it has no rule" (emphasis added). However, the excerpt fails to disclose "determining whether a user confirms the activation of the policies" (emphasis added) or "activating the policies if the user confirms" (emphasis added), as claimed by applicant.

In the Office Action mailed 10/12/2006, the Examiner argues that "when a rule in ConSeal has not been used before and the system is in Checked Learning Mode, the user is prompted to make a rule for the packet (i.e. allow or disallow) thereby creating two inactive policies (one to allow the packet and one to disallow the packet)" and "[t]herefore when the user selects an action the user is activating one of the previous inactive rules."

Applicant respectfully disagrees. Simply nowhere in the excerpt relied on by the Examiner is there any disclosure that "when the user selects an action the user is activating one of the previous inactive rules," as the Examiner notes. In fact, applicant points out that ConSeal actually teaches that "[t]he system manages rulesets activation...behind the scenes" (see page 1), which clearly *teaches away* from "determining whether a user confirms the activation of the policies" (emphasis added) or "activating the policies if the user confirms" (emphasis added), as claimed by applicant.

In addition, applicant respectfully asserts that ConSeal merely discloses that "Checked Learning Mode prompts the user for rule generation when it encounters a packet for which it has no rule" (emphasis added). Clearly, prompting a user for rule generation when no rule exists, as in ConSeal, fails to even suggest "determining whether a user confirms the activation of the policies" (emphasis added) and "activating the policies if the user confirms" (emphasis added), as claimed by applicant. Applicant respectfully asserts that ConSeal's prompt for "rule generation" for a packet which has no rule simply fails to teach "determining whether a user confirms the activation of the policies" (emphasis added) or "activating the policies if the user confirms" (emphasis added), as claimed by applicant. Clearly, rule generation, as in ConSeal, fails to meet "activating the policies," in the manner as claimed by applicant.

Again, since at least the first and third elements of the *prima facie* case of obviousness have not been met, especially in view of the amendments made hereinabove, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 33-36 below, which are added for full consideration:

"wherein the associated conditions of the policies dictate the manner in which the active policies are to be deactivated" (see Claim 33);

"determining whether one of the active policies is still active including determining whether the condition associated with the active policy is still met" (see Claim 34);

"de-activating the active policy if the associated condition is not met and determining whether the de-activated policy is to be reused or discarded" (see Claim 35); and

"wherein an indication of the determination whether the de-activated policy is to be reused or discarded is stored with the associated condition " (see Claim 36).

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P048).

Respectfully submitted,
Zilka-Kotab, PC.

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100